**ABSTRACT**

Using information applied to a packet at an ingress port of a network for enhancing security such as user authentication for example. Such authentication may be applied in addition to (i.e., as an extension of) other authentication measures. The information applied to a packet may be "context information" which replaces at least some bits of layer 2 information (e.g., a header). Users or customers may define security policies. They may define different security policies for different types of transactions. They may also define security policies based on the location from which the transaction originated. If the customer is an organization with different classes of users, it may define different security policies based on the type of transaction, the location from which the transaction originated, and/or the class of user. The class of user may be identified based on at least a part of the "context information". At least a part of the context information may also be used to monitor a location from which a transaction originated, thereby permitting fraudulent uses to be traced.